CLAIM AMENDMENTS

Claims 1 and 22-28 are pending, wherein claim 1 is currently amended herein, claims 2-21 have been deleted and claims 22-28 are newly added.

1. (Currently amended) A MAC (media access control) address-based communication restricting method using access vectors stored in address tables, wherein the access vectors indicate whether two nodes, corresponding to a MAC source address and a MAC destination address, may access each other, the method comprising the steps of:

receiving packet data upon request of communication through at least one port of a plurality of ports of an Ethernet switch;

reading a MAC destination address and a MAC source address included in the received packet data;

detecting, in [[an]] the address table, access vectors corresponding to the MAC destination and source addresses; and

denying access if the access vectors of the MAC destination and source addresses are not matched.

Claims 2 through 21 (canceled)

22. (New) A packet switch communication method, comprising the steps of:

receiving packet data upon request of communication through at least one port of a plurality of ports of said packet switch ;

reading a MAC (media access control) destination address and a MAC (media access control) source address included in said received packet data;

determining whether said received MAC source address is stored in an address table having an access vector indicating whether allowance for access of client nodes is made or not, wherein each client node is identified by at least corresponding MAC address;

when it is determined that said received MAC source address is stored in said address table, determining whether an access vector corresponding to said received MAC destination address is matched with an access vector corresponding to said received MAC source address, wherein both of the access vectors are stored in said address table;

if the access vectors corresponding to said received MAC destination and source addresses are matched, transmitting said received packet data to a MAC destination address; and

denying access if said access vectors of said received MAC destination and source addresses are not matched.

23. (New) The method as set forth in claim 22, further comprising steps of :

configuring an anti-hacker table comprising information pertaining to a plurality of the client nodes and a plurality of server nodes of a network, wherein each server node is identified by at least corresponding MAC address;

when it is determined that said received MAC source address is not stored in said address table, determining whether information corresponding to said received MAC source address is stored in said anti-hacker table; and

when it is determined that said received MAC source address is stored in said anti-hacker

table, modifying an access vector in said MAC source address to a security key, to thereby store the modified address in the said address table.

24. (New) The method as set forth in claim 23, further comprising steps of :

adding a port number, corresponding to the port through which said packet data was received, to a storage area corresponding to said MAC source address received in said anti-hacker table.

25. (New) A packet switch communication method, comprising the steps of :

receiving packet data upon request of communication through at least one port of a plurality of ports of said packet switch;

reading a MAC (media access control) destination address and a MAC (media access control) source address included in said received packet data;

determining whether said received MAC source address is stored in an address table having an access vector indicating whether allowance for access of client nodes is made or not, wherein each client node is identified by at least corresponding MAC address;

when it is determined that said received MAC source address is not stored in said address table determining whether information corresponding to said received MAC source address is stored in said anti-hacker table; and

when it is determined that said received MAC source address is stored in an anti-hacker table, modifying an access vector in said MAC source address to a security key, to thereby store the modified address in the said address table, said anti-hacker table comprising information pertaining to a plurality of said client nodes and a plurality of server nodes of a network, wherein each server

node is identified by at least corresponding MAC address.

26. (New) A MAC (media access control) address-based communication restricting packet switch comprising:

a plurality of MAC ports;

a data exchange for establishing paths of packet data between MAC ports

a packet memory storing an address table having access vector indicating whether allowance for access of client nodes is made or not, wherein each client node is identified by at least corresponding MAC address;

a transmission/reception controller controlling data exchange;

wherein said transmission/reception controller reads a MAC destination address and a MAC source address included in said received packet data from MAC ports, transmits said received packet data to a MAC destination address when said received MAC source address is stored in said address table and if an access vector corresponding to said received MAC destination address is matched with an access vector corresponding to said received MAC source address, denies access if said access vectors of said received MAC destination and source addresses do not match.

27. (New) A MAC address-based communication restricting packet switch communication method as set forth in claim 26,

when said received MAC source address is not stored in the address table, and if information corresponding to the received MAC source address is stored in an anti hacker table, modifying an access vector in said MAC source address to a security key, to thereby store the modified address

in the said address table, wherein said anti-hacker table comprise information pertaining to a plurality of client nodes and a plurality of sever nodes, wherein each server node is identified by at least corresponding MAC address.

28. (New) A MAC address-based communication restricting packet switch communication method as set forth in claim 27, wherein said transmission/reception controller adds a port number, corresponding to the MAC port through which said data packet was received, to a storage area corresponding to said received MAC source address in said anti-hacker table.